

← imagine this is me

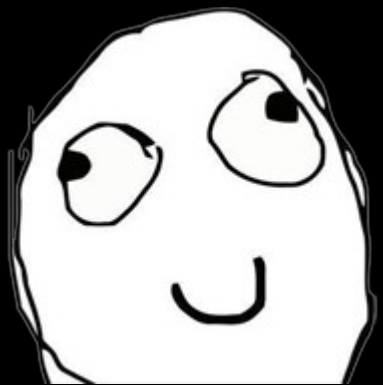
## Wats dat?

- Packstation
  - A “service” by DHL used widely in Germany
  - Basically a P/O box
  - Send DHL (and only DHL) packets to a packstation
  - Pick it up whenever you want



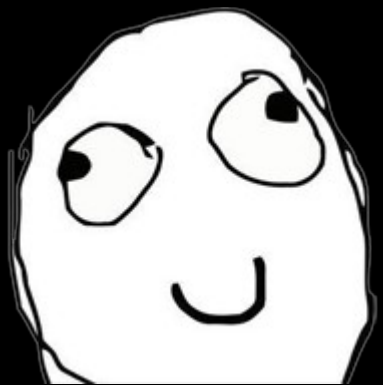
## How Does it Work?

- Packstation lets you login with
  - Magstripe + PIN
  - Card Number + PIN



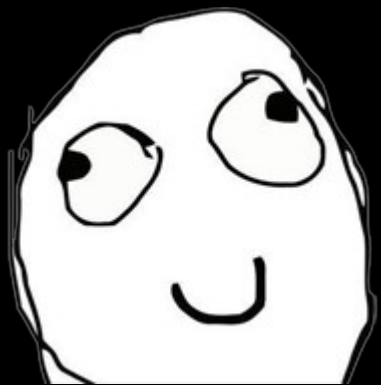
## How Does it Work?

- Packstation lets you login with
  - Magstripe + PIN
  - Card Number + PIN ← teh awesome!



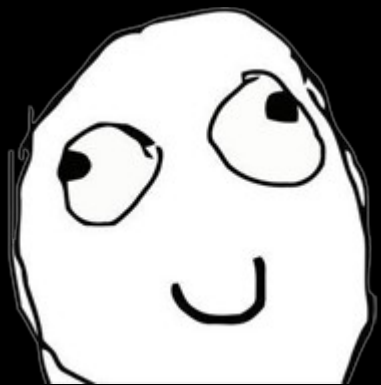
## A Little History

- Signed up for Packstation
- Used it plenty (→ Amazon <3)
- Lost my card T\_T
- Used just the number & PIN to log in :3
- But “suddenly” ...



## A Little History

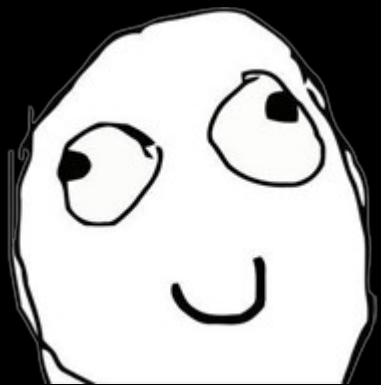
- Signed up for Packstation
- Used it plenty (→ Amazon <3)
- Lost my card T\_T
- Used just the number & PIN to log in :3
- But “suddenly” ...





## A Little History

- Signed up for Packstation
- Used it plenty (→ Amazon <3)
- Lost my card T\_T
- Used just the number & PIN to log in :3
- But “suddenly” ...




## A Little History

*... card required for login!!1*



## A Little History

Eine neue PACKSTATION-Sendung ist für Sie da (Kundenkarte zur Abholung mitnehmen!)  | x



DHL to me


[show details](#) Jun 1

 Reply



Okay, not so suddenly... who reads mail anyway

## A Little History

Eine neue PACKSTATION-Sendung ist für Sie da (Kundenkarte zur Abholung mitnehmen!)  | x



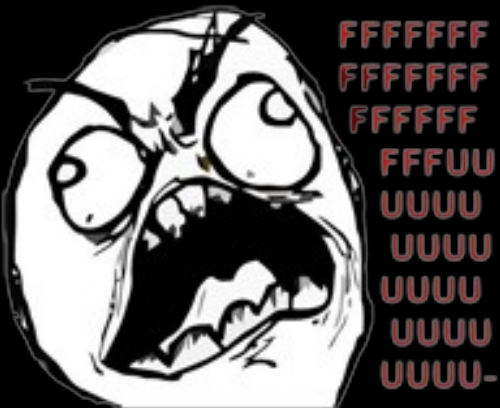
DHL to me

[show details](#) Jun 1

[Reply](#)

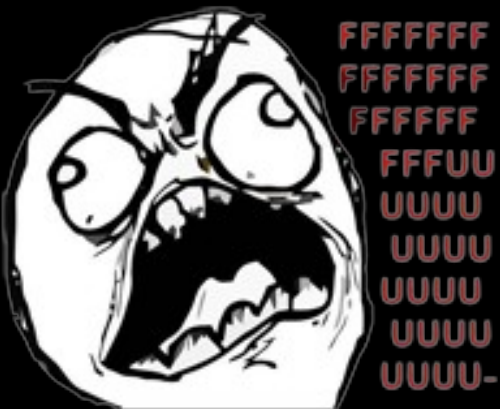


Okay, not so suddenly... who reads mail anyway



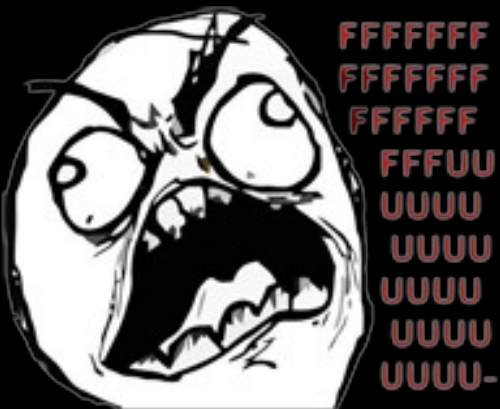
## A Little History

- Called Packstation support
- Raged
- ...
- No profit (claimed it protects from phishing)
- But got a new card



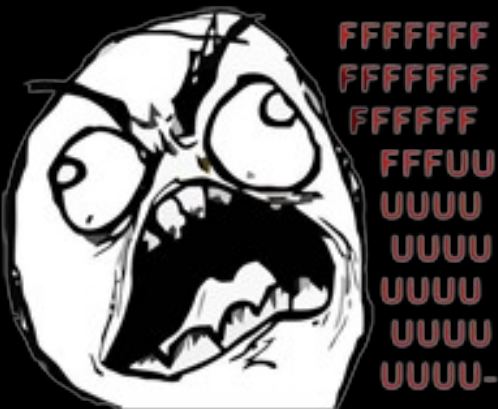
## A Little History

- Called Packstation support
- Raged
- ...
- No profit (claimed it protects from phishing)
- But got a new card



## A Little History

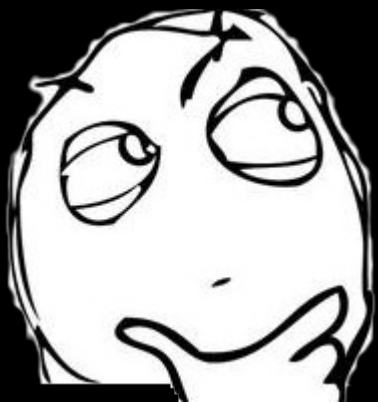
- Called Packstation support
- Raged
- ...
- No profit (claimed it protects from phishing)
- But got a new card



Same number ... and pin ...

## A Little History

- Called Packstation support
- Raged
- ...
- No profit (claimed it protects from phishing)
- But got a new card

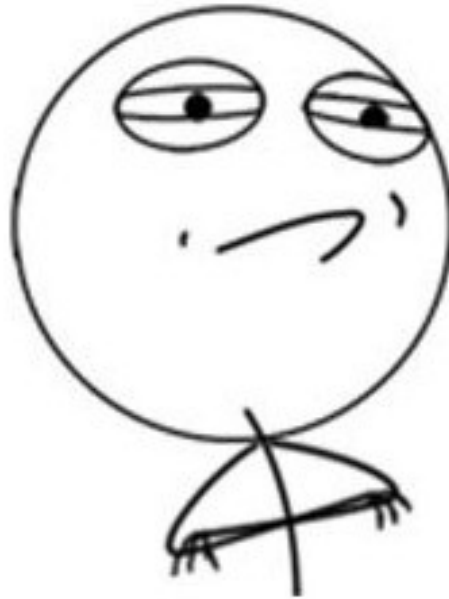


Same number ... and pin ...





**CHALLENGE ACCEPTED**



## How to Read a Magstripe

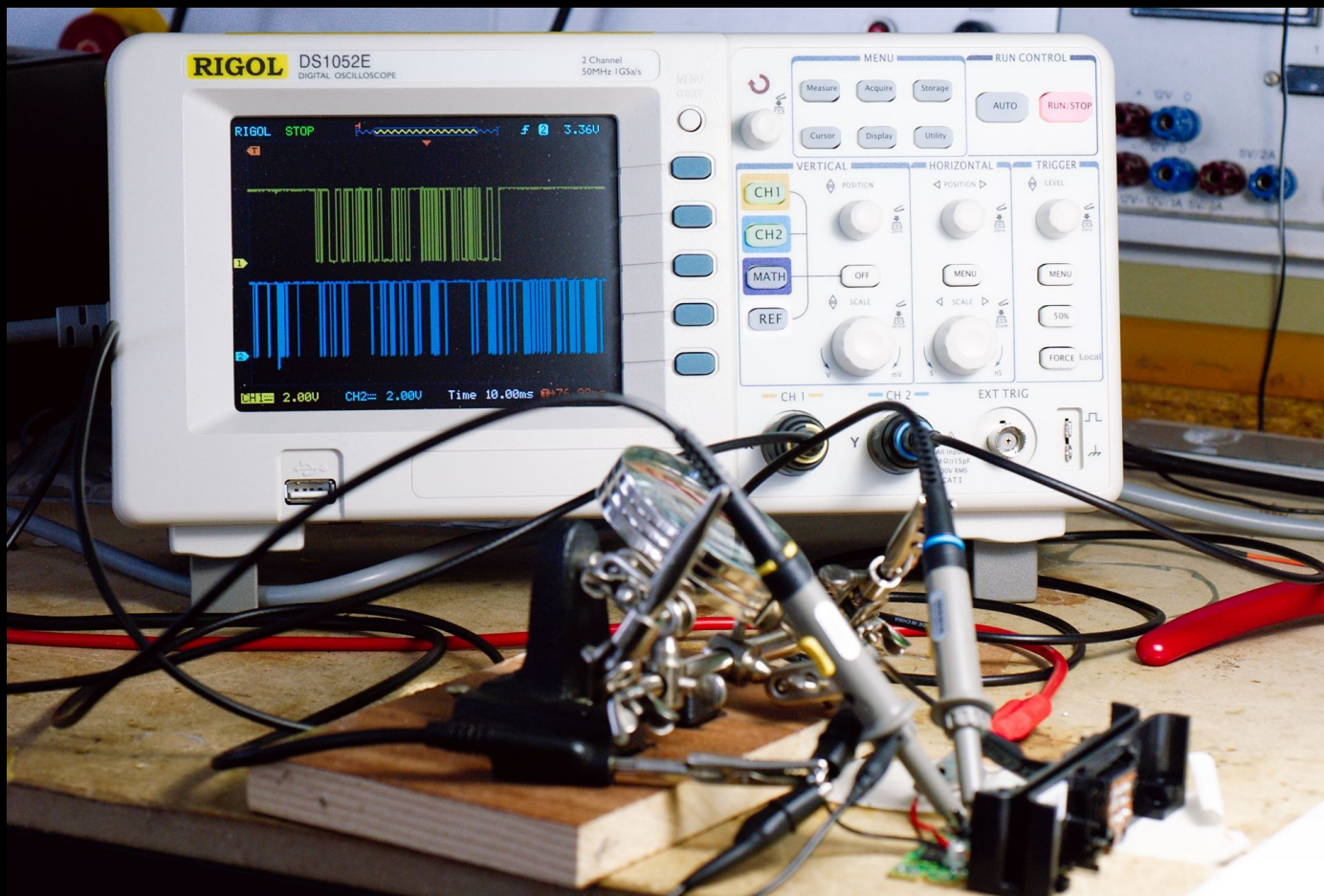
- When in doubt... C4!





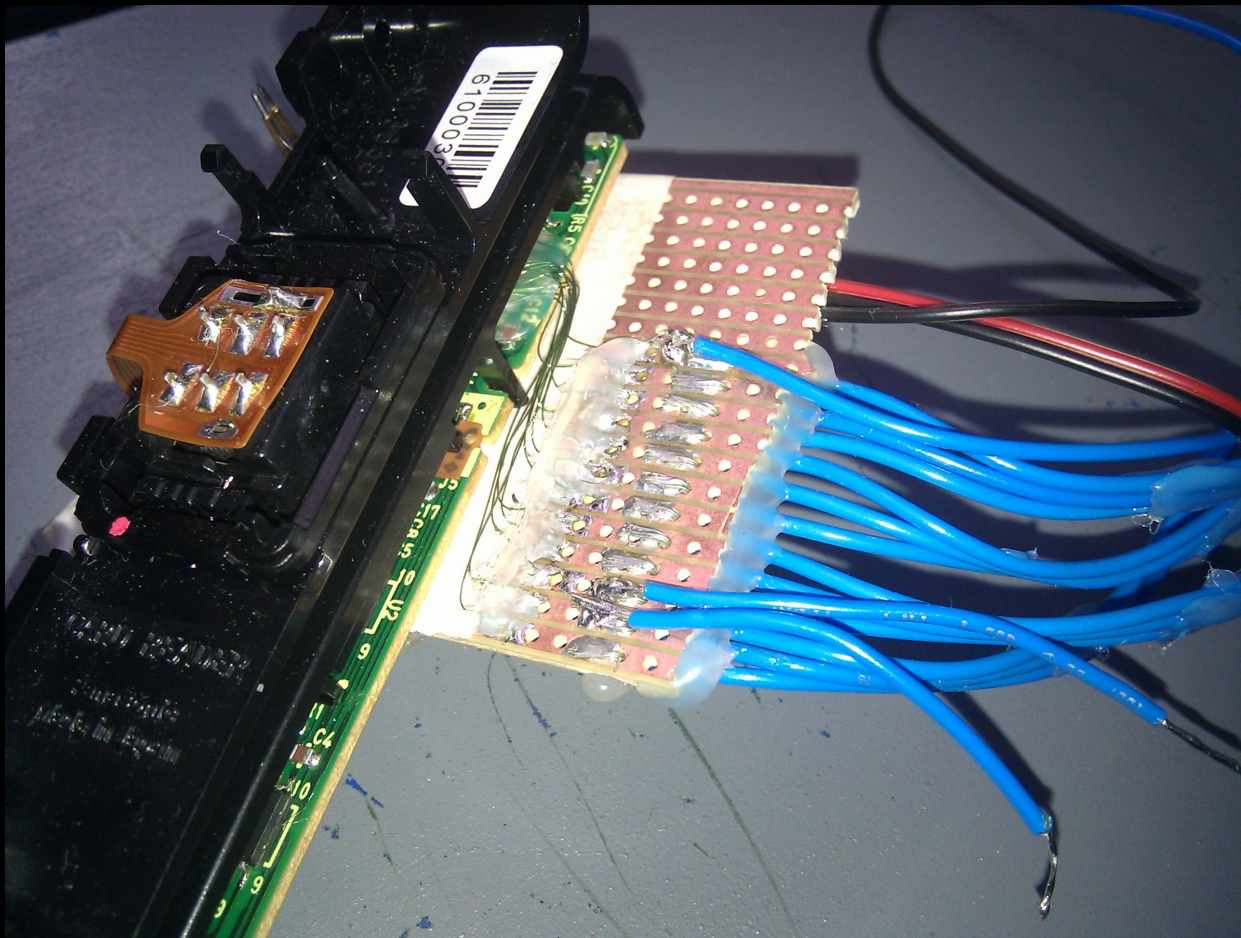
## How to Read a Magstripe

- When in doubt... SCOPE!



## How to Read a Magstripe

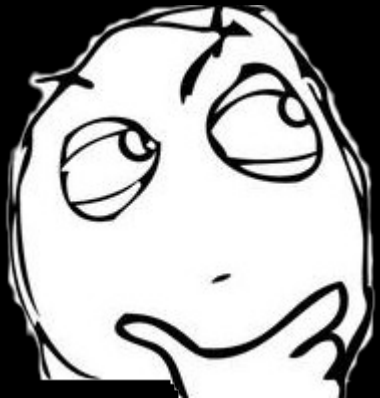
- Just for blog-creds: Hook it up to an Arduino





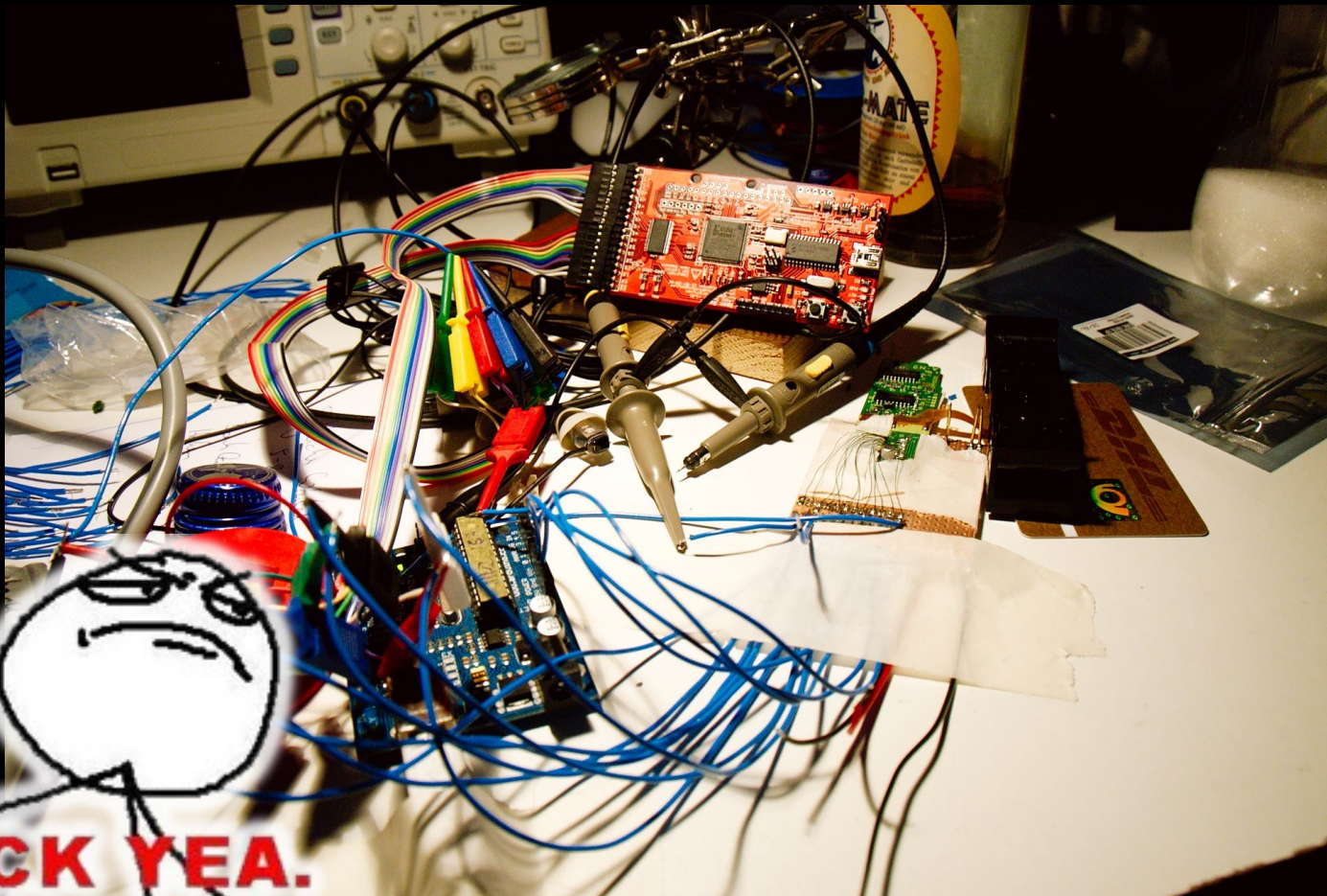
## How to Read a Magstripe

- Or maybe not...
- Turns out it's too slow for this kind of reader :(



## How to Read a Magstripe

- OpenBench Logic Sniffer!



## What's on That Thing?



## What's on That Thing?

*\*drumroll\**

## What's on That Thing?



#\$%&ing plaintext!

## The Actual Data

- Track 1: Your Name
- Track 2: Your Card ID
- Track 3: 00590000000000000000000000000000

## The Actual Data

- Track 1: Your Name
- Track 2: Your Card ID
- Track 3: 0059000...

Get it from: your shipping address

## The Actual Data

- Track 1: Your Name
- Track 2: Your Card ID
- Track 3: 0059000...

Get it from: your shipping address (again)

## The Actual Data

- Track 1: Your Name
- Track 2: Your Card ID
- Track 3: 0059000...

Get it from: nowhere. Always the same.

## The Actual Data

- Track 1: Your Name
- Track 2: Your Card ID
- Track 3: 0059000...



Get it from: nowhere. Always the same.

## Using a Logic Sniffer

- Pro
  - Very versatile
  - Let's you grab plenty of channels
  - +5 offense against hardware
- Contra
  - Not really practical :(
  - Doesn't actually *write* cards :(((



## Using a Logic Sniffer

- Pro
  - Very versatile
  - Let's you grab plenty of channels
  - +5 offense against hardware
- Contra
  - Not really practical :(
  - Doesn't actually *write* cards :(((

But... Proof of Concept, Baby!



OPERATOR: WE GET SIGNAL.

CAPTAIN: WHAT ?

*So now I have to get a proper writer.*

## Toys and Stuff

- Turns out writers are expensive :(
- Around 250, 500,... 1000 EUR

## Toys and Stuff

- Turns out writers are expensive :(
- Around 250, 500,... 1000 EUR
- All writers? Nah...

## Toys and Stuff

- Turns out writers are expensive :(
- Around 250, 500,... 1000 EUR
- All writers? Nah...
- China to the rescue!

150 EUR later...

☆ [redacted] to me

[show details](#) May 18

[Reply](#)

hi, my dear friend,

thank you for your msg, we will ship the item to you by dhl.

it will arrive you soon, could you pls kindly offer me your phone number ?

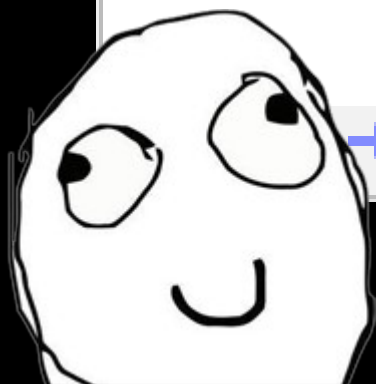
pls don't worry, it is just for the shipping company use it. because they need this phone number before

ship the item, thank you for your understanding.

waiting for your reply

- Show quoted text -

[Forward](#)





[show details](#) May 18



r msg, we will ship the item to you by dhl.

oon, could you pls kindly offer me your phone number ?

t is just for the shipping company use it. because they need this phone

nk you for your understanding.

eply

[ward](#)

[show details](#) May 18

we will ship the item to you by dhl.

could you pls kindly offer me your phone number ?

for the shipping company use it. because they need this

for your understanding.

[show details](#) May 18



r msg, we will ship the item to you by dhl.

oon, could you pls kindly offer me your phone number ?

t is just for the shipping company use it. because they need this phone

nk you for your understanding.

eply

[ward](#)

☆ [redacted] to me

[show details](#) May 18

[Reply](#)

hi, my dear friend,

thank you for your msg, we will ship the item to you by dhl.

it will arrive you soon, could you pls kindly offer me your phone number ?

pls don't worry, it is just for the shipping company use it. because they need this phone number before

ship the item, thank you for your understanding.

waiting for your reply





[redacted] to ping

[show details](#) May 18

[Reply](#)



On Wed, May 18, 2011 at 9:28 AM, [redacted]

> hi, my dear friend,

Hi,

> thank you for your msg, we will ship the item to you by dhl.

> it will arrive you soon, could you pls kindly offer me your phone number ?

> pls don't worry, it is just for the shipping company use it. because they

> need this phone number before

Oh, that would be perfect! if you're shipping by DHL, can you please ship it to the following address instead:



Packstation

Baden-Württemberg

and

ackstation which would allow me to pick the package up the day.

number is [+49](#) [redacted]



## What Now?

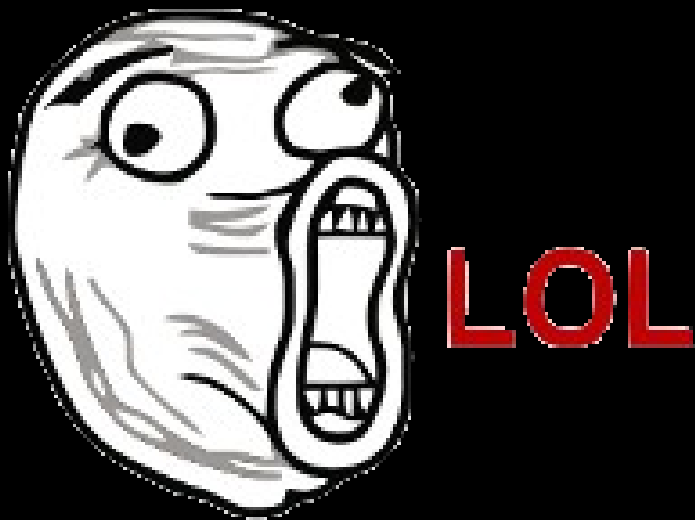
- For minute, let's assume we're phishing.
- This is, after all, what using the card should protect you against.

## What Now?

- For minute, let's assume we're phishing.
- This is, after all, what using the card should protect you against.

## What Now?

- For minute, let's assume we're phishing.
- This is, after all, what using the card should protect you against.





## What we Need

- A name
- A number
- Another number
- A PIN

## What we Need

- A name got it! (address)
- A number
- Another number
- A PIN

## What we Need

- A name got it! (address)
- A number got it! (address)
- Another number
- A PIN

## What we Need

- A name got it! (address)
- A number got it! (address)
- Another number got it! (always the same)
- A PIN

## What we Need

- A name got it! (address)
- A number got it! (address)
- Another number got it! (always the same)
- A PIN got it! (remember, phishing)

## Let's get to Work!

- Phish some! (I'll just phish myself)
- Clone^W backup a card. (my own)
- ...
- Profit



# HACKSTATION®



2011-06-25 GPN11 (v1.1)

hackstation – 15 minutes of packet rage

## Results

- The name field is totally irrelevant



## Results

- The name field is totally irrelevant
  - ... says Bobby Tables

## Results

- The name field is totally irrelevant
  - ... says Bobby Tables
- Modifying track 3 doesn't do a thing

## Results

- The name field is totally irrelevant
  - ... says Bobby Tables
- Modifying track 3 doesn't do a thing
- Number + PIN is checked online

## Results

- The name field is totally irrelevant
  - ... says Bobby Tables
- Modifying track 3 doesn't do a thing
- Number + PIN is checked online
  - Packstation keeps greeting me with my full name

## Results

- The name field is totally irrelevant
  - ... says Bobby Tables
- Modifying track 3 doesn't do a thing
- Number 1 is checked online
  - Password keeps greeting me with my full name



## What now?

- Added security?

## What now?

- Added security?
  - Nil, Null, Nada

## What now?

- Added security?
  - Nil, Null, Nada
  - It's actually worse! → False sense of security!



## What now?

- Added security?
  - Nil, Null, Nada
  - It's actually worse! → False sense of security!
- If you're smart enough to phish...

## What now?

- Added security?
  - Nil, Null, Nada
  - It's actually worse! → False sense of security!
- If you're smart enough to phish...
  - ... you're smart enough to clone a card.

## What now?

- Added security?
  - Nil, Null, Nada
  - It's actually worse! → False sense of security!
- If you're smart enough to phish...
  - ... you're smart enough to clone a card.
  - Costs: 150 EUR → nothing



## Meta

- Thanks
  - @momorientes - for the Pollin card reader
  - @dop3j0e – logic sniffer and perl foo
- Contact
  - hadez@shackspace.de
  - @hdznrrd
- Slides
  - <http://bit.ly/m0MAF9>